The Listing of Claims will replace all prior versions and listings of claims in the present patent application:

LISTING OF CLAIMS

Claims 1-11 (Canceled)

12. (Currently Amended) A method for fast generation of a cryptographic key, comprising:

generating a first public key for encrypting a first wireless communication; ~~and~~

generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication, wherein the second public key is independent of the first public key; and

determining whether the second public key has been stored prior to establishing the second wireless communication.

13. (Cancelled)

14. (Previously Presented) The method of claim 13, further comprising:

using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

15. (Previously Presented) The method of claim 13, further comprising:

generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

16. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

means for generating a first public key for encrypting a first wireless communication; ~~and~~

means for generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication, wherein the second public key is independent of the first public key; and

means for determining whether the second public key has been stored prior to establishing the second wireless communication.

17. (Cancelled).

18. (Previously Presented) The wireless communication device of claim 17, further comprising:

means for using the second public key to encrypt the second wireless communication when it is determined that the second public key has been stored.

19. (Previously Presented) The wireless communication device of claim 17, further comprising:

means for generating a third public key to encrypt the second wireless communication when it is determined that the second public key has not been stored.

20. (Currently Amended) A wireless communication device for fast generation of a cryptographic key, comprising:

a processor for generating a first public key to encrypt a first wireless communication and generating, upon termination of the first wireless communication, a second public key for use in a second wireless communication; and

a memory for storing the second public key,

wherein the second public key is independent of the first public key and further

wherein the processor determines whether the second public key has been stored prior to establishing the second wireless communication.

21. (New) A processor for fast generation of a cryptographic key, said processor being configured to:

generate a first public key for encrypting a first wireless communication;

generate, upon termination of the first wireless communication, a second public key for use in a second wireless communication, wherein the second public key is independent of the first public key; and

determine whether the second public key has been stored prior to establishing the second wireless communication.

22. (New) A computer program product comprising instructions for fast generation of a cryptographic key, wherein the instructions upon execution cause a computer to:

generate a first public key for encrypting a first wireless communication;

generate, upon termination of the first wireless communication, a second public key for use in a second wireless communication, wherein the second public key is independent of the first public key; and

determine whether the second public key has been stored prior to establishing the second wireless communication.